Qualys Context XDR (Extended Detection and Response)

Oracle OCI Loadbalancer

Data Mapping Guide

February 13, 2023

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Thank you for your interest in Extended Detection and Response (XDR). Qualys Context XDR expands the capabilities of the Qualys Cloud Platform to integrate data points from other Qualys products offer a unified view of your organization’s security posture. Context XDR integrates data points (events/logs) from your enterprise’s ecosystem that comprises of several heterogenous sources. This data is normalized, enriched and then categorized before storing it in the Qualys Context XDR data model. This unified database that holds data points from multiple security applications is then used to offer a 360° view of your organization’s security posture — all from a single solution.

The Data Mapping Guides provide a list of the fields received through a data source and how these fields are mapped to the Context XDR data model.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at http://www.qualys.com/support/.

Overview

Qualys Context Extended Detection and Response (XDR) can be configured to ingest data from several different data sources. Each data source has its own data points, and this Data Mapping Guide offers insight into how these data points are interpreted, normalized, and mapped in Qualys Context XDR.

This guide focuses on the data mapping between Oracle OCI Loadbalancer fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys XDR UI, navigate to **Configuration** > **Data Collection** > **Catalog**. If the source you are looking for is not in the catalog, you can add a request for support using the **Not in the list?** card.

Device Details

- **Device Type** – Loadbalancer
- **Device Vendor** – Oracle
- **Device Product** – Oracle OCI Loadbalancer
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Oracle OCI Loadbalancer using the following formats:

- **Cloud**

For information on configuring collectors, refer to the Deploying a Collector section in the Online Help.

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Loadbalancer
deviceVendor – Oracle

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
data.backendAddr	destinationIpv4	10.245.3.27	IP address of the backend server, which processed the client request.
	destinationPort	5432	Port number of the backend server, which processed the client request.
data.backendConnectTime	Oracle_LB_BackendConnectTime	0.001	Time spent (in seconds, with millisecond precision), to establish backend server connection.
data.clientAddr	sourceIpv4	10.246.21.55	IP address of the requesting client.
	sourcePort	52556	Port Number of the requesting client.
data.lbStatusCode	status	502	Status code of the response from the load balancer.
data.sslCipher	Oracle_LB_SSLCipher	ECDHE-RSA-AES256-GCM-SHA384	Negotiated SSL cipher between the client and the load balancer.
data.sslProtocol	Oracle_LB_SSLProtocol	TLSv1.2	Negotiated SSL protocol between the client and the load balancer.
id	externalId	387ac59c-0637-4d69-ab0c-93f763af9348-access-2422230	Associated ID given in the event by the event source.
oracle.compartmentid	Oracle_CompartmentId	ocid1.compartment.oc2..aaaaaaaa6uc2paylaw4jiwpth6s4j7ytqebkymaqlvcpe4qepjaj7ecwag6a	OCID of the compartment the log group is in.
oracle.ingestedtime	receivedTime	2022-09-12T12:44:40.549Z	Time the log was ingested by OCI Logging.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
oracle.loggroupid	Oracle_LogGroupId	ocid1.loggroup.oc2.us-langley-1.amaaaaaauasve7iadyjeyvbq76epixiifdp622p2z7szvdbasdeekbpkfkmq	OCID of the log group.
oracle.logid	Oracle_LogId	ocid1.log.oc2.us-langley-1.amaaaaaauasve7ia4b3zm5p44dlqt7dl4iieldkpkjtudufwx4ihifp5ti4q	OCID of the log
oracle.tenantid	Oracle_TenantId	ocid1.tenancy.oc2..aaaaaaaapgk4wliefejurazpv4onobar6tm6gwon3pkmtcufnusm3b6v2ska	OCID of the tenant.
time	eventTime	2022-09-12T12:44:39.055Z	Event Time when log was logged
type	eventType	com.oraclecloud.loadbalancer.access	Type of the event.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Loadbalancer
DeviceModel	Oracle OCI Loadbalancer
DeviceVendor	Oracle
DeviceHost	-
CustomerId	d656b196-edb7-45e6-8485-3748a740d002
CollectorId	ae102769-bd05-415d-af3c-2cc59681cbab
EventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
EventId	d656b196-edb7-45e6-8485-3748a740d002
CollectorReceivedTime	Jun 01, 2021 11:29:04 AM